Vorlesung "Logische Grundlagen"

LG6: Äquivalenzrelationen

Stichworte: Ä-Relation, Ä-Klassen, Quotientenmengen, solche mit algebraischen Strukturen + ·, Konstruktion der Zahlbereiche mit Ä-Relationen

---

§1: Ä-Relationen und Ä-Klassen

Def.: Sei X eine Menge. Eine Relation $R \subseteq X \times X$ in X heißt eine Äquivalenzrelation (hier kurz: Ä-Rel.), wenn sie

- reflexiv (7): $\forall x \in X: xRx$
- symmetrisch (8): $\forall x, y \in X: xRy \Rightarrow yRx$
- und transitiv (12): $\forall x, y, z \in X: xRy \wedge yRz \Rightarrow xRz$

ist (vgl. LG5).

Übliche Zeichen für Ä-Relationen sind $\sim, \simeq, \equiv, \cong, \approx$, etc.
(die in bestimmten Kontexten aber meist auch speziellere Bedeutungen haben).
Wir wollen hier $\sim$ für eine Ä-Relation schreiben, also $x \sim y$ für $(x,y) \in R$.
"Tilde"

Beispiele: 1. "=" Gleichheit bei Mengen, Zahlen, Geraden, ...
2. "ist gleich alt wie" in der Menge der Menschen
3. "ist im gleichen Bierkasten" in der Menge der Bierflaschen
4. "ist parallel zu" in der Menge der Geraden
5. "ist kongruent zu" in der Menge der Strecken
6. "hat gleiche Parität wie" in $\mathbb{N}_0$ [n, m haben dieselbe Parität, wenn sie beide gerade oder beide ungerade sind]
7. "hat dieselbe Richtung und Länge" in der Menge der Pfeile in der Ebene
8. "hat dieselbe Krümmung wie" in der Menge der Bananen

Jede Ä-Rel. $\sim$ in X zerlegt X in paarweise disjunkte, nichtleere Teilmengen, auch Klasseneinteilung genannt:

Def.: Die Menge aller zu $x \in X$ bzgl. $\sim$ in Relation stehenden Elemente von X heißt Äquivalenzklasse und wird mit $[x]$ bezeichnet, d.h. $[x] := \{y \in X \mid y \sim x\}$

Andere Notationen: $[\![x]\!]$, $\underline{x}$, $\bar{x}$, $\llcorner x \lrcorner$, ...

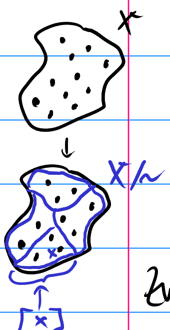
Bem.: • $[x]$ ist demnach die Äquivalenzklasse, die x enthält: $x \in [x]$, so dass $[x] \neq \emptyset$ folgt ⌜denn $\sim$ ist reflexiv⌟

• Es gilt: $\forall x,y \in X: \; x \sim y \Leftrightarrow [x] = [y]$ (obwohl hier $x \neq y$ gelten kann!)

⌜„$\Rightarrow$": Sei $x \sim y$. Zu „$\subseteq$": ist $z \in [x]$, folgt $z \sim x$, mit $x \sim y$ folgt aus der Transitivität $z \sim y$, also ist $z \in [y]$. Zu „$\supseteq$": analog.

„$\Leftarrow$": Sei $[x] = [y]$. Dann ist $x \in [x] = [y]$, also $x \sim y$.⌟

• Es gilt: $\forall x,y,z \in X: \; z \in [x] \wedge z \in [y] \Rightarrow [x] = [y]$. (Da $x \sim z \sim y$, also $x \sim y$.)



Umformuliert: $(\forall z \in X: z \in [x] \cap [y] \Rightarrow [x] = [y])$

$$\Leftrightarrow \neg\left(\exists z \in X: z \in [x] \cap [y] \wedge [x] \neq [y]\right)$$

$$\Leftrightarrow \neg\left([x] \cap [y] \neq \emptyset \wedge [x] \neq [y]\right)$$

$$\Leftrightarrow \left([x] \neq [y] \Rightarrow [x] \cap [y] = \emptyset\right)$$

Zwei verschiedene Ä-Klassen sind also disjunkt, d.h. ihr Durchschnitt ist $\emptyset$.

(Anders ausgedrückt: Jedes Element z gehört zu genau einer Ä-Klasse.)

• Die Vereinigung aller Ä-Klassen ergibt X, d.h. $X = \bigcup_{x \in X} [x]$.

⌜„$\subseteq$": Ist $x \in X$, folgt $x \in [x]$, also $x \in$ r.S., „$\supseteq$": klar⌟

• Obige Überlegungen zeigen: $x \sim y \Leftrightarrow [x] = [y] \Leftrightarrow [x] \cap [y] \neq \emptyset$.

Eine Ä-Rel. erzeugt also eine neue Menge, die Menge aller Ä-Klassen:

Def.: Sei $\sim$ eine Ä-Rel. in X. Dann heißt

$$X/\sim \; := \{[x] \mid x \in X\}$$

(sprich "X modulo $\sim$", auch "X durch $\sim$")

die Quotientenmenge von X nach $\sim$.

• Ein (jedes) El. $y \in [x]$ heißt Repräsentant der Klasse $[x]$.

• Eine Menge $\mathcal{R} \subseteq X$ heißt vollständiges Repräsentantensystem von $X/\sim$, wenn $\mathcal{R}$ genau ein Element jeder Klasse von $X/\sim$ enthält.

Beispiele: in obigen Beispielen 1.–8. haben wir:

1. Ä-Kl.: Die für jedes x zugehörige Ä-Klasse ist $[x]=\{x\}$.
   Also: $X/\sim \;=\{\{x\}\mid x\in X\}$ ⇝ könnte mit X identifiziert werden, denn kriegen nichts Neues! Weiter: Nur $Q=X$ ist vollst. Repr.system.
2. Alle Menschen mit gleichem Lebensjahr bilden jeweils eine Ä-Klasse.
3. Die Bierkästen sind genau die Ä-Klassen.
   ⌈Tatsächlich erzeugt jede Partition $X=\dot{\bigcup}_{i=1}^{n} X_i$ (alle $X_i\neq\emptyset$, und $\forall i\neq j: X_i\cap X_j=\emptyset$) von X eine Ä-Rel. $\sim$ in X durch $x\sim y :\Leftrightarrow \exists i\in\{1,\dots,n\}: x\in X_i \wedge y\in X_i$.⌋
4. Alle Geraden mit gleicher Richtung gehören zu einer Ä-Klasse. Man kann sagen, über die Parallelität/Ä-Klassenbildung kann "Richtung" erklärt werden.
5. Alle Strecken mit gleicher Länge gehören zu einer Ä-Klasse. Man kann sagen, über die Kongruenz/Ä-Klassenbildung kann "Länge" erklärt werden. (Alle zum "Urmeter" gleichlangen Stäbe sind 1m lang per Definition...)
6. Haben $\mathbb{N}_0/\sim \;=\{\mathcal{G},\mathcal{U}\}$, wo $\mathcal{G}=\{2n\mid n\in\mathbb{N}_0\}$ die geraden und $\mathcal{U}=\{2n+1\mid n\in\mathbb{N}_0\}$ die ungeraden Zahlen sind.
   Haben insb. $\mathbb{N}_0=\mathcal{G}\,\dot{\cup}\,\mathcal{U}$. Bem.: Wir können mit El. von $\mathbb{N}_0/\sim$ "rechnen":

   erklären dies repräsentantenweise: ← $\begin{cases}\mathcal{G}+\mathcal{G}:=\mathcal{G},\ \mathcal{G}+\mathcal{U}:=\mathcal{U}+\mathcal{G}:=\mathcal{U},\ \mathcal{U}+\mathcal{U}=\mathcal{G}\\ \mathcal{G}\cdot\mathcal{G}:=\mathcal{G},\ \mathcal{G}\cdot\mathcal{U}:=\mathcal{U}\cdot\mathcal{G}:=\mathcal{G},\ \mathcal{U}\cdot\mathcal{U}=\mathcal{U}\end{cases}$

   Haben ja: $\mathcal{G}=[0]$, $\mathcal{U}=[1]$,
   und $[0]+[0]:=[0]$, aber auch $[4]+[6]:=[10]=[0]\dots$
   und $[0]+[1]:=[1]$, aber auch $[4]+[7]:=[11]=[1]\dots$
   usw. Werden diese Idee später etwas vertiefen.
   (Nennen $\mathbb{N}_0/\sim$ auch $\mathbb{F}_2$ ⇝ 2-elementiger Körper.)
7. Die Ä-Klassen sind die Vektoren, welche jeweils durch einen Pfeil repräsentiert werden, der vom Ursprung aus beginnt. Diese repräsentierenden Pfeile werden durch ihren Endpunkt an der Pfeilspitze dargestellt, den wir mit einem Tupel angeben.
8. Alle Bananen gleicher Krümmung gehören zu einer Ä-Klasse. Den Begriff "Krümmung" kann man mit Mitteln der Analysis präzisieren.

Gerade das Bsp. 6. zeigt neue interessante Strukturen (mit $+, \cdot$) auf, wollen es vertiefen/verallgemeinern. Dies zunächst in einem weiteren Bsp.:

9. Statt mit "gerade/ungerade" wollen wir mit den Resten "rechnen", die wir bei Division natürlicher Zahlen durch $M=12$ erhalten:
Betr. $X=\mathbb{N}_0$ und

$n \sim m :\Leftrightarrow n$ und m lassen denselben Rest bei Division durch 12
$\Leftrightarrow 12 \mid n-m \ \vee \ 12 \mid m-n$
$\Leftrightarrow \exists k \in \mathbb{N}_0: n = m+12k$ oder $m = n+12k$

Dann ist also $[0]=[12]=[24]=\ldots=\{0,12,24,\ldots\}$ (alle mit Rest 0)
$[1]=[13]=[25]=\ldots=\{1,13,25,\ldots\}$ (alle mit Rest 1)
$\vdots$
$[11]=[23]=[47]=\ldots=\{11,23,\ldots\}$ (alle mit Rest 11)

$\leadsto$ identifizieren die Ä-Klassen mit den 12 möglichen Resten $0, 1, \ldots, 10, 11$.

Haben: $\{0,1,\ldots,11\}$ ist vollst. Repr.system, aber auch z.B. $\{12,1,\ldots,9,10,23\},\ldots$

Somit: $\mathbb{N}_0/\sim \ = \underbrace{\{[0],[1],\ldots,[11]\}}_{\text{diese Darstellung der Ä-Klassen gefällt uns am besten.}} = \{[12],[1],\ldots,[10],[23]\},\ldots$

"Rechnen" mit Resten (d.h. mit Ä-Klassen, den El. von $\mathbb{N}_0/\sim$) erklären wir <u>repräsentantenweise</u>: $[k]+[l] := [k+l]$
$[k]\cdot[l] := [k\cdot l]$

für $k,l \in \mathbb{N}_0$ (!). Wir haben hier die Def. von "+", "$\cdot$" auf $\mathbb{N}_0/\sim$ von k,l abhängig gemacht, obwohl wir doch nur $[k]$, $[l]$ miteinander verknüpfen wollten; prinzipiell könnte je nach Repräsentantenwahl ein anderes Ergebnis nach der Verknüpfung herauskommen. Tut es hier aber nicht! Denn: Es ist egal, welche Repräsentanten wir wählen für $[k], [l]$,
sagen wir mal $[k]=[u]$ und $[l]=[v]$,
dann ist nämlich $[k+l]=[u+v]$.

müsste man genauer begründen...

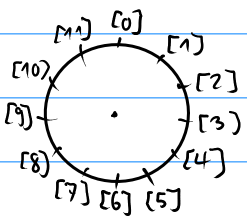
$\ulcorner \cdot\ k \sim u \Leftrightarrow \exists r \in \mathbb{N}_0: k-u = 12r \ \vee\ u-k = 12r$, sei OE die 1. Alternative w,
$\cdot\ l \sim v \Leftrightarrow \exists s \in \mathbb{N}_0: l-v = 12s \ \vee\ v-l = 12s$, sei OE die 1. Alternative w.
Somit: $k+l \sim u+v$, denn $k+l-(u+v) = (k-u)+(l-v) = 12(r+s)$. $\lrcorner$

Eine ähnliche Überlegung zeigt $[k\cdot l] = [u \cdot v]$.

Man sagt, aufgrund dieser Rechnung ist die gegebene Def. von $+, \cdot$ auf den Ä-Klassen in $\mathbb{N}_0/\sim$ repräsentantenunabhängig und deswegen wohldefiniert.

auch: "mod 12"

In diesem Beispiel sprechen wir vom Rechnen/der Arithmetik modulo 12.
(Die Zahl $M=12$ könnte auch durch einen anderen Modul M ersetzt werden.)
Anschaulich ist die Arithmetik mod 12 das Rechnen mit Stunden auf einer Uhr:



$[2]+[6]=[8]$

$[9]+[4]=[13]=[1]$

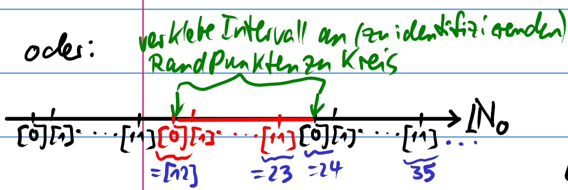
$[11]+[11]=[22]=[10], \ldots$

$[13]+(-[5])=[8], \ldots$ usw.

↳ erkläre $-[5]$ als die Klasse mit $(-[5])+[5]=0$, d.h. $-[5]=[7]$

$[13]+[7]=[20]=[8] \quad \ldots$

oder:



Diese Verknüpfungen $+, \cdot$ auf $\mathbb{N}_0/\sim$ haben viele neue interessante Eigenschaften.

§2: Konstruktion der Zahlbereiche

Ä-Relationen werden sehr vielfältig eingesetzt, um neue mathematische Strukturen zu definieren (z.B. Quotientenvektorräume, Quotientenkörper, Randverklebungen...).
Eine Hauptanwendung ist die Konstruktion der Zahlbereiche $\mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, die wir hier angeben (natürlich gibt es viele andere Möglichkeiten, dies zu tun):

(1.) $\mathbb{Z} := \mathbb{N}_0 \times \mathbb{N}_0 / \sim$ mit der Ä-Relation

$$(n,m) \sim (u,v) \;:\Longleftrightarrow\; n+v = m+u.$$ ("$n-m$ = Konstante" ...)

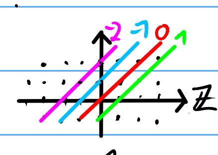
Darin ist $\mathbb{N}_0$ eingebettet in der Form $\{[(n,0)] \mid n \in \mathbb{N}_0\}$.

Weiter: $[(n,m)] + [(u,v)] := [(n+u, m+v)]$.

Die Zahl $-n$ für $n \in \mathbb{N}_0$ liegt vor als $[(0,n)]$,

denn $[(n,0)] + [(0,n)] = [(n,n)] = [(0,0)]$.

Ü Wie geht die Definition von "$\cdot$" und "$\leq$"? (nicht naheliegend!)
Welche Eigenschaften haben $+, \cdot$ und $\leq$?



Bei der Konstruktion spielt nur der 1. Quadrant $\mathbb{N}_0 \times \mathbb{N}_0$ eine Rolle!

(2.) $\mathbb{Q} := \mathbb{Z} \times \underset{\text{ohne } 0}{\mathbb{N}} / \sim$ mit der Ä-Relation

$$(z,n) \sim (y,m) \;:\Leftrightarrow\; zm = ny$$

Darin ist $\mathbb{Z}$ eingebettet in der Form $\{ [(z,1)] \mid z \in \mathbb{Z} \}$.
Wir schreiben dann $\frac{z}{n}$ für $[(z,n)]$ und erhalten die üblichen Rechengesetze für $+, \cdot$, wenn wir erklären:

$$\frac{z}{n} \cdot \frac{y}{m} := \frac{zy}{nm}, \qquad \frac{z}{n} + \frac{y}{m} := \frac{zm + yn}{nm}.$$

Def. $\leq$: $\frac{z}{n} \leq \frac{y}{m} :\Leftrightarrow zm \leq yn$.

(3.) $\mathbb{R} := \mathcal{C}/\sim$ mit der Menge

$$\mathcal{C} := \{ (a_n)_{n\in\mathbb{N}} \subseteq \mathbb{Q} \mid \underbrace{(a_n) \text{ ist Cauchyfolge in } \mathbb{Q}}_{\forall \varepsilon > 0\ \exists N_\varepsilon\ \forall n,m \geq N_\varepsilon:\ |a_n - a_m| < \varepsilon} \}$$

und der Ä-Relation $(a_n)_{n\in\mathbb{N}} \sim (b_n)_{n\in\mathbb{N}} :\Leftrightarrow (a_n - b_n)_{n\in\mathbb{N}}$ ist Nullfolge.
$\Leftrightarrow \forall \varepsilon > 0\ \exists N_\varepsilon\ \forall n \geq N_\varepsilon: |a_n - b_n| < \varepsilon$

<u>Satz</u>: Der Körper der reellen Zahlen ist "der" (bis auf Isomorphie) eindeutig bestimmte vollständige angeordnete Körper.

<u>Def.</u>: • Ein Körper K (mit Verknüpfungen $+, \cdot$) und einer strikten Anordnung "$<$" (oder Anordnung) (die trichotomisch (13) und transitiv (12) ist) heißt <u>angeordneter Körper</u>, falls $\forall x,y,z \in K: x<y \Rightarrow x+z < y+z$ (Monotonie der Addition)
und $\forall x,y,z \in K: x<y, z>0 \Rightarrow xz < yz$ (Monotonie der Multiplikation) gilt.

• Ein angeordneter Körper heißt <u>archimedisch angeordnet</u>, falls
$\forall x \in K\ \forall y \in K, y>0\ \exists n \in \mathbb{N}: ny > x$.
(Dies ist genau dann der Fall, wenn die "natürlichen Zahlen in K" nicht beschränkt sind.)

<u>Satz</u>: Für angeordnete Körper K sind äquivalent: (D.h.: (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3) $\Leftrightarrow$ (4).)
(1) Jede nichtleere, nach oben beschr. Teilmenge von K besitzt ein Supremum in K.
(2) Jede monoton wachsende, nach oben beschr. Folge aus K konvergiert in K.
dies erfüllt $\mathbb{R}$ laut obiger Konstruktion (und damit auch (1), (2) und (4).) → (3) K ist archimedisch und jede Cauchyfolge aus K konvergiert in K.
(4) K ist archimedisch und im Durchschnitt jeder IVschachtelung liegt genau ein El. von K.
⌜Eine Intervallschachtelung ist eine Folge abgeschlossener, ineinander verschachtelter Intervalle, deren Länge gegen Null geht.⌟

<u>Def.</u>: Ein angeordneter Körper K heißt <u>vollständig</u>, falls (1) ⌜$\Leftrightarrow$(2)$\Leftrightarrow$(3)$\Leftrightarrow$(4)⌟ gilt.

Bem.: Wegen obigem Satz, dass $\mathbb{R}$ als vollständiger angeordneter Körper im wesentlichen eindeutig bestimmt ist, kann man auch mit der Charakterisierung von $\mathbb{R}$, d.h. den Körperaxiomen plus dem "Vollständigkeitsaxiom", meist in der Form (1), beginnen und damit Analysis betreiben, ohne je eine Konstruktion von $\mathbb{R}$ zu benutzen. Denn die explizit konstruierten Elemente von $\mathbb{R}$ – entweder Ä-Klassen von Cauchyfolgen, unendlich lange Dezimalbrüche, ... sind zu kompliziert zum damit Rechnen/Aufschreiben.

(4.) $\mathbb{C} := \mathbb{R}^2$ mit
$$(x,u)+(y,v):=(xy+uv)$$
$$(x,u)\cdot(y,v):=(xy-uv,\ xv+uy)$$
ist die einfachste Konstruktion von $\mathbb{C}$. Es gibt viele andere, eine andere ist diese:

$\mathbb{C} := \mathbb{R}[X]/\sim$ mit den reellen Polynomen $\mathbb{R}[X] := \{\sum_{i=0}^{m} a_i X^i \mid m \in \mathbb{N}_0, a_i \in \mathbb{R}\}$

und der Ä-Relation $f(X)\sim g(X) :\Leftrightarrow \exists\, h(X)\in\mathbb{R}[X]:$
$$f(X)-g(X) = h(X)\cdot(X^2+1).$$

$\rightsquigarrow$ die Ä-Klassen sind El. von $\mathbb{C}$ und wir erklären $+,\cdot$ durch

$$(*)\ \left\{\begin{array}{l}[f(X)]+[g(X)] := [f(X)+g(X)]\\ [f(X)]\cdot[g(X)] := [f(X)\cdot g(X)]\end{array}\right.$$ ← deutlich natürlichere Def.!

Jede Klasse $[f(X)]$ enthält genau ein Polynom der Form $a_0 + a_1 X$ ist also durch ein Zahlenpaar (a_0, a_1) eindeutig bestimmt, die wieder auf Real- und Imaginärteil führen.

Beachten Sie:
$[X^2+1] = [0]$, und weiter ist
$$[X]\cdot[X] = [X^2] = [X^2+1-1] = [X^2+1]+[-1] = [-1],$$
d.h. $[X]$ ist eine Zahl mit $[X]^2 = [-1]$,
die würden wir ja wohl "i" nennen...

Bem. zum Schluss: Oft vererben sich Eigenschaften von "+", "·" auf Quotientenmengen, wenn diese wie in $(*)$ erklärt werden, wie z.B. Assoziativität etc., aber nicht immer. Deswegen sind Beweise erforderlich.